In the Claims:

Please withdraw claims 35-39.

1. (Previously presented): A security system for allowing a client to access a protected resource through an application container, the security system comprising:

an application container, which provides services for a protected resource, wherein the application container delegates authorization decisions to the security service by passing an access request and a callback handler to the security service when the application container receives an access request for a protected resource from a client;

context information, wherein the context information comprises one or more parameter values describing the access request and can be retrieved from the application container by the security service using the callback handler;

said security service for making a decision to permit or deny the access request, wherein the security service includes a plurality of security providers that may be plugged into the security service, and wherein the plurality of security providers use the callback handler to request context information from the application container for the access request, and wherein depending on output from each security provider the security service determines entitlements for the client to use with the protected resource;

said security service is located at a first computer, and said protected resource is located either at the same first computer or at a second computer; and

a resource interface for communicating permitted access requests to said protected resource.

2. (Previously Presented): The security system of claim 1 wherein the application container of claim 1 reads an application deployment description and registers the application deployment description within the security service.

3. (Canceled)

4. (Previously Presented): The security system of claim 2 wherein the application container is a Web Application container.

5. (Previously Presented): The security system of claim 1 wherein the security service includes a plurality of access decision mechanisms for defining an access policy and each of the plurality of access decision mechanism can determine its own contributory decision to permit, deny, or abstain from the access request.

6. (Previously Presented): The security system of claim 5 wherein the security service further includes an access controller for transferring the access request to the plurality of access decision mechanisms, and for combining the contributory decisions into an overall decision by the security service to permit or deny the access request.

7. (Previously Presented): The security system of claim 5 wherein one or more of the plurality of the access decision mechanisms represent a business function related access policy.

8. (Original): The security system of claim 5 wherein access decisions may be added to the security service to reflect changes in the access policy.

9. (Previously Presented): The security system of claim 5 wherein the plurality of the access decision mechanisms are used to define the entitlements for the client to access the protected resource.

10. (Previously Presented): The security system of claim 5 wherein a deny or abstain by any one of the plurality of access decision mechanisms causes the security service to deny the access request.

11. (Previously Presented): The security system of claim 5 wherein an abstain by any one of the plurality of access decision mechanisms does not cause the security service to deny the access request.

12. (Previously Presented): The security system of claim 5 wherein the security service further includes an audit mechanism for auditing the determinations of the plurality of access requests.

13. (Previously Presented): The security system of claim 1 wherein the resource interface includes an interface mechanism to pass access requests to or from a protected resource.

14. (Canceled)

15. (Previously Presented): The security system of claim 13 wherein the interface mechanism includes a security provider interface.

16. (Previously Presented): The security system of claim 13 wherein the interface mechanism is included as a plug-in into the resource interface.

17. (Previously Presented): The security system of claim 1 wherein the security service further makes a decision on whether to permit or deny a response to the access request from the protected resource to the client.

18. (Previously presented): A method of allowing a client to access a protected resource through an Application Container, the method comprising:

receiving at an application container, which provides services to the resources it contains, an access request from said client to access said protected resource;

communicating the access request from the application container to a security service with the access request and a callback handler, wherein the application container delegates authorization decisions to the security service by passing an access request and a callback handler to the security service when the application container receives an access request for a protected resource from a client;

making a decision at the security service to permit or deny the access request, wherein the security service includes a plurality of security providers that may be plugged into the security service;

using the callback handler at each security provider to request context information from the application container for the access request, wherein the context information comprises one or more parameter values describing the access request and can be retrieved from the application container by the security service using the callback handler;

determining entitlements for the client to use with the protected resource depending on output from each security provider; and

communicating a permitted access request through a resource interface to the protected resource.

19. (Currently Amended): The method of claim 18 wherein the application container of claim 18 reads an application deployment description and registers the deployment description within the security service.

20. (Canceled)

21. (Previously Presented): The method of claim 19 wherein the application container is a Web Application container.

22. (Previously Presented): The method of claim 18 further comprising:

defining an access policy via a plurality of access decision mechanisms within the security service; and,

determining at each access decision mechanism a contributory decision to permit, deny, or abstain from the access request.

23. (Previously Presented): The method of claim 22 further comprising:

transferring via an access controller the access request to the plurality of access decision mechanisms, and combining the contributory decisions into an overall decision by the security service to permit or deny the access request.

24. (Previously Presented): The method of claim 22 wherein one or more of the plurality of the access decision mechanisms represent a business function related access policy.

25. (Original): The method of claim 22 wherein access decisions may be added to the security service to reflect changes in the access policy.

26. (Previously Presented): The method of claim 22 further comprising:

using the plurality of access decision mechanisms to define entitlements for the client to access the protected resource.

27. (Previously Presented): The method of claim 22 wherein a deny or abstain by any one of the plurality of access decision mechanisms causes the security service to deny the access request.

28. (Previously Presented): The method of claim 22 wherein an abstain by any one of the plurality of access decision mechanisms does not cause the security service to deny the access request.

29. (Previously Presented): The method of claim 22 further comprising:

auditing via an audit mechanism the determinations of the plurality of access decision mechanisms.

30. (Previously Presented): The method of claim 18 wherein the step of communicating the access request includes passing access requests via an interface mechanism to or from a protected resource.

31. (Canceled)

32. (Previously Presented): The method of claim 30 wherein the interface mechanism includes a security provider interface.

33. (Previously Presented): The method of claim 30 wherein the interface mechanism is included as a plug-in into the resource interface.

34. (Previously Presented): The method of claim 18 further comprising:

making a decision on whether to permit or deny a response to the access request from the protected resource to the client.

35. (Withdrawn): A method for determining user entitlements to access protected resources in a secure environment, comprising:

receiving an access request from a user application to access a protected resource, by invoking a security service with the access request and a callback;

determining user entitlements to access the protected resource, wherein the determining includes polling a plurality of security providers that may be plugged into the security service, and wherein the plurality of security providers use a callback handler to request context information from an application container for the access request;

making a decision at the security service based on the user entitlements to permit or deny the access request; and

the steps of either

(a) communicating a permitted access request to the protected resource, or

(b) denying a denied access request to the protected resource.

36. (Withdrawn): The method of claim 35 wherein if the access request is permitted, user entitlements also determine a type of access available to a user of the protected resource.

37. (Withdrawn): The method of claim 36 wherein the type of access includes any of view, modify, delete, or copy, any part or all of the protected resource.

38. (Withdrawn): The method of claim 35 wherein information about user entitlements can be communicated from a first security realm to a second security realm.

39. (Withdrawn): The method of claim 38 wherein additional information from a first security realm can be used to modify the user entitlements, prior to communicating the information about user entitlements from the first security realm to the second security realm.

40. (Previously Presented): The security system of claim 1, wherein entitlements comprise at least one of business logic and functionality entitlements.

41. (Canceled)